

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

P/2238-28
#3
8-31-01
J1033 U.S. PRO
09/858433
05/16/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出願年月日

Date of Application:

2000年 5月17日

出願番号

Application Number:

特願2000-144234

出願人

Applicant(s):

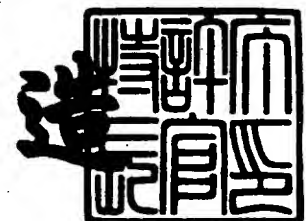
日本電気株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 4月13日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2001-3028878

【書類名】 特許願

【整理番号】 49220150

【提出日】 平成12年 5月17日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/46

【発明者】

 【住所又は居所】 東京都港区芝五丁目7番1号 日本電気株式会社内

 【氏名】 川上 弘幸

【特許出願人】

 【識別番号】 000004237

 【氏名又は名称】 日本電気株式会社

【代理人】

 【識別番号】 100088812

 【弁理士】

 【氏名又は名称】 ▲柳▼川 信

【手数料の表示】

 【予納台帳番号】 030982

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 通信装置及び通信制御方法並びに制御プログラム記録媒体

【特許請求の範囲】

【請求項 1】 プロバイダ網上にトンネルを形成することにより、複数のカスタマ網間の通信のための仮想専用線（VPN）を構築するようにした通信システムにおいて、前記トンネルの入出力端に接続されたエッジ通信装置であって、前記カスタマ網内で使用されるルーティングプロトコルを終端する終端手段を含むことを特徴とするエッジ通信装置。

【請求項 2】 前記仮想専用線に関する VPN 構築情報と、前記プロバイダ網に接続され予めカプセルアドレスが割り当てられたポートと前記カスタマ網側の各通信装置の IP アドレスとの対応情報とからなるテーブルを更に含み、

前記終端手段は、前記カスタマ網から入力されたパケットの宛先アドレスから前記テーブルを検索する検索手段と、この検索されたカプセルアドレスを基に前記パケットをカプセル化して前記プロバイダ網へ送出するカプセル化手段とを有することを特徴とする請求項 1 記載のエッジ通信装置。

【請求項 3】 前記カプセル化手段は、同一の仮想専用線に属する他のカスタマ網に対して、前記カプセルアドレスを基に前記制御パケットをカプセル化して送出するようにしたことを特徴とする請求項 2 記載のエッジ通信装置。

【請求項 4】 前記終端手段は、前記カスタマ網内の IP アドレスの追加やトポロジの変化に应答して前記カスタマ網で生成される制御パケットを受信解読する手段と、この解読結果に従って前記テーブルのデータ更新を行う手段とを有することを特徴とする請求項 2 または 3 記載のエッジ通信装置。

【請求項 5】 前記終端手段は、前記プロバイダ網から自装置に到着したパケットに対して前記カプセルアドレスが含まれるカプセルを外し、当該パケットに含まれる宛先 IP アドレスを基に前記テーブルから送出先を決定して送出する手段を有することを特徴とする請求項 2 ～ 4 いずれか記載のエッジ通信装置。

【請求項 6】 前記終端手段は、前記カスタマ網に対する現用インタフェースの障害に应答してこの障害インタフェースに関連する前記テーブル内の情報を

削除すると共に、関連する他のエッジ通信装置へ障害通知及び予備インタフェースの通知をなす手段を有することを特徴とする請求項 2～5 いずれか記載のエッジ通信装置。

【請求項 7】 前記終端手段は、他のエッジ通信装置からの障害通知に応答して前記障害インタフェースに関連する前記テーブル内の情報を削除すると共に、前記予備インタフェースの通知に応答して前記テーブル内にこの予備インタフェースに関連する情報を追加する手段を有することを特徴とする請求項 6 記載のエッジ通信装置。

【請求項 8】 前記カスタマ網内で使用されるルーティングプロトコルは、O S P F (Open Shortest Path First) プロトコルであることを特徴とする請求項 1～7 いずれか記載のエッジ通信装置。

【請求項 9】 プロバイダ網上におけるエッジ通信装置間にてトンネルを形成することにより、複数のカスタマ網間の通信のための仮想専用線 (V P N) を構築するようにした通信システムにおける通信制御方法であって、前記エッジ通信装置において、前記カスタマ網内で使用されるルーティングプロトコルを終端する終端ステップを含むことを特徴とする通信制御方法。

【請求項 1 0】 前記エッジ通信装置には、前記仮想専用線に関する V P N 構築情報と、前記プロバイダ網に接続され予めカプセルアドレスが割り当てられたポートと前記カスタマ網側の各通信装置の I P アドレスとの対応情報とからなるテーブルが設けられており、

前記終端ステップは、前記カスタマ網から入力されたパケットの宛先アドレスから前記テーブルを検索する検索ステップと、この検索されたカプセルアドレスを基に前記パケットをカプセル化して前記プロバイダ網へ送出するカプセル化ステップとを有することを特徴とする請求項 9 記載の通信制御方法。

【請求項 1 1】 前記カプセル化ステップは、同一の仮想専用線に属する他のカスタマ網に対して前記カプセルアドレスを基に前記制御パケットをカプセル化して送出するようにしたことを特徴とする請求項 1 0 記載の通信制御方法。

【請求項 1 2】 前記終端ステップは、前記プロバイダ網から自装置に到着したパケットに対して前記カプセルアドレスが含まれるカプセルを外し、当該パ

ケットに含まれる宛先 I P アドレスを基に前記テーブルから送出先を決定して送出するステップを有することを特徴とする請求項 1 0 または 1 1 記載の通信制御方法。

【請求項 1 3】 前記終端ステップは、前記カスタマ網内の I P アドレスの追加やトポロジの変化に応答して前記カスタマ網で生成される制御パケットを受信解読するステップと、この解読結果に従って前記テーブルのデータ更新を行うステップとを有することを特徴とする請求項 1 0 ～ 1 2 いずれか記載の通信制御方法。

【請求項 1 4】 前記終端ステップは、前記カスタマ網との現用インタフェースの障害に応答してこの障害インタフェースに関連する前記テーブル内の情報を削除すると共に、関連する他のエッジ通信装置へ障害通知及び予備インタフェースの通知をなすステップを有することを特徴とする請求項 1 0 ～ 1 3 いずれか記載の通信制御方法。

【請求項 1 5】 前記終端ステップは、他のエッジ通信装置からの障害通知に応答して前記障害インタフェースに関連する前記テーブル内の情報を削除すると共に、前記予備インタフェースの通知に応答して前記テーブル内にこの予備インタフェースに関連する情報を追加するステップを有することを特徴とする請求項 1 4 記載の通信制御方法。

【請求項 1 6】 前記カスタマ網内で使用されるルーティングプロトコルは、O S P F (Open Shortest Path First) プロトコルであることを特徴とする請求項 9 ～ 1 5 いずれか記載の通信制御方法。

【請求項 1 7】 前記テーブルを集中管理する集中処理装置が設けられており、前記制御パケットの解読結果に従って前記テーブルのデータ更新後に、この更新されたテーブルを前記集中処理装置へアップロードするステップと、前記集中処理装置からこのアップロードされたテーブルに関連するエッジ通信装置にダウンロードするステップとを含むことを特徴とする請求項 1 3 記載の通信制御方法。

【請求項 1 8】 プロバイダ網上におけるエッジ通信装置間にてトンネルを形成することにより、複数のカスタマ網間の通信のための仮想専用線 (V P N)

を構築するようにした通信システムにおける通信制御方法のプログラムを記録した記録媒体であって、

前記プログラムは、前記エッジ通信装置において、前記カスタマ網内で使用されるルーティングプロトコルを終端する終端ステップを含むことを特徴とする記録媒体。

【請求項 1 9】 前記エッジ通信装置には、前記仮想専用線に関する V P N 構築情報と、前記プロバイダ網に接続され予めカプセルアドレスが割り当てられたポートと前記カスタマ網側の各通信装置の I P アドレスとの対応情報とからなるテーブルが設けられており、

前記終端ステップは、前記カスタマ網から入力されたパケットの宛先アドレスから前記テーブルを検索する検索ステップと、この検索されたカプセルアドレスを基に前記パケットをカプセル化して前記プロバイダ網へ送出するカプセル化ステップとを有することを特徴とする請求項 1 8 記載の記録媒体。

【請求項 2 0】 前記カプセル化ステップは、同一の仮想専用線に属する他のカスタマ網に対して前記カプセルアドレスを基に前記制御パケットをカプセル化して送出するようにしたことを特徴とする請求項 1 9 記載の記録媒体。

【請求項 2 1】 前記終端ステップは、前記プロバイダ網から自装置に到着したパケットに対して前記カプセルアドレスが含まれるカプセルを外し、当該パケットに含まれる宛先 I P アドレスを基に前記テーブルから送出先を決定して送出するステップを有することを特徴とする請求項 1 9 または 2 0 記載の記録媒体。

【請求項 2 2】 前記終端ステップは、前記カスタマ網内の I P アドレスの追加やトポロジの変化に応答して前記カスタマ網で生成される制御パケットを受信解読するステップと、この解読結果に従って前記テーブルのデータ更新を行うステップとを有することを特徴とする請求項 1 9 ～ 2 1 いずれか記載の記録媒体。

【請求項 2 3】 前記終端ステップは、前記カスタマ網に対する現用インタフェースの障害に応答してこの障害インタフェースに関連する前記テーブル内の情報を削除すると共に、関連する他のエッジ通信装置へ障害通知及び予備インタ

フェースの通知をなすステップを有することを特徴とする請求項 1 9 ～ 2 2 いずれか記載の記録媒体。

【請求項 2 4】 前記終端ステップは、他のエッジ通信装置からの障害通知に応答して前記障害インタフェースに関連する前記テーブル内の情報を削除すると共に、前記予備インタフェースの通知に応答して前記テーブル内にこの予備インタフェースに関連する情報を追加するステップを有することを特徴とする請求項 2 3 記載の記録媒体。

【請求項 2 5】 前記カスタマ網内で使用されるルーティングプロトコルは、O S P F (Open Shortest Path First) プロトコルであることを特徴とする請求項 1 8 ～ 2 4 いずれか記載の記録媒体。

【発明の詳細な説明】

【0 0 0 1】

【産業上の利用分野】

本発明は通信装置及び通信制御方法並びに制御プログラム記録媒体に関し、特にプロバイダ網上にトンネルを形成することにより、複数のカスタマ網間の通信のための仮想専用線 (V P N) を構築するようにした通信方式に関するものである。

【0 0 0 2】

【従来の技術】

カプセル化技術を用いた V P N (Virtual Private Network) 構築技術に関して、シスコ (Cisco) 社から、プロバイダ網に M P L S (Multi Protocol Label Switch) を用いた通信方式が提案されている。このような V P N 技術について説明する。V P N とは、インターネット等の公衆通信網上で、論理的なグループを形成し、かつそのグループ間で閉域性を保つ機能を設けたネットワークをいう。このインターネット等の公衆通信網には、通常不特定多数のユーザが接続しており、そのために基本的には特定のユーザだけの通信はできず、第三者による不正アクセスは避けられないというセキュリティ上の問題がある。

【0 0 0 3】

そこで、近年エンドーエンドでセキュリティ対策を施すことにより、インター

ネット上に仮想的に専用線を構築し、LAN (Local Area Network) 間接続の基幹回線として利用するVPN技術が注目されている。具体的には、エンドーエンドでのデータの暗号化、ユーザ認証及びアクセス制御等のセキュリティを施した上で、特定の拠点間をインターネットを介して接続し、閉域性のあるグループを提供するものである。

【 0 0 0 4 】

かかるVPNを公衆通信網上に実現することで、特定ユーザだけの通信が可能となり、インターネット等を仮想的な専用網として利用することができるのである。この様なVPN方式に関しては、特開平10-70566号公報、特開平11-355272号公報等の開示のものがある。

【 0 0 0 5 】

図16はこの様なVPNを使用した通信システムの概略ブロック図である。図16において、LAN等の閉域性のあるグループであるカスタマ網A1～A3と、インターネット等のプロバイダ網C1とがある。カスタマ網A1はカスタマ通信装置（以下、通信装置のことを単にノードと称する）11～13を有しており、また、カスタマ網A2はカスタマノード21～23を有しており、更にカスタマ網A3はカスタマノード31～33を有している。そして、プロバイダ網C1には、カスタマ網との境界にエッジノード41～43が設けられており、境界以外にはコアノード44、45が設けられている。尚、図16では、カスタマ網A1との境界にエッジノード41が、カスタマ網A2、A3との境界にエッジノード42が、それぞれ設けられているものとする。

【 0 0 0 6 】

この場合、カスタマ網A1とA2、A3との間の通信は、エッジノード間に構築されたトンネル51により形成されたVPNによって行われるが、このときのルーティングのためのプロトコルの関係は図示のようになっている。すなわち、LAN等のカスタマ網A1～A3では、インテリアルルーティングプロトコルであるIGP (Interior Gateway Protocol) が用いられ、プロバイダ網C1では、IBGP (Interior Border Gateway Protocol) が用いられ、これ等網間のインタフェース部分では、EBGP (Exterior Border Gateway Protocol) が用いら

る。

【 0 0 0 7 】

【発明が解決しようとする課題】

従来のVPN通信方式の問題点としては、図16に示したLAN等の閉域性のあるグループであるカスタマ網A1～A3と、インターネット等のプロバイダ網C1との境界では、EBGPが使用されているので、カスタマノードとエッジノードとに対してBGP (Border Gateway Protocol) による通信ができるように設定する必要がある。これは、カスタマノードにBGPを実装する必要があるばかりではなく、サービスを受けるカスタマがBGPの知識が必要となり、負荷の増大を招くという欠点がある。

【 0 0 0 8 】

また、このようなVPN方式では、カスタマ網とプロバイダ網との境界でEBGPが使用されているので、カスタマ網とプロバイダ網との間で、いわゆるマルチホーミング構成を構築することができない。従って、例えば、帰属するエッジノードが停止した場合や、帰属するインタフェース部分にリンク断が生じた場合には、配下のカスタマ網の通信停止を引き起こし、信頼性の低下につながるという欠点がある。

【 0 0 0 9 】

更に、プロバイダ網であるMPLS網をプロバイダ網C1内部でVPN毎の経路情報がBGPで伝達されるので、カスタマ網内で使用されるルーティングプロトコルであるOSPF (Open Shortest Path First) のOSPF情報が透過的に通らず、結果としてOSPFドメインが分断されることになる。特に、ATM (非同期通信モード) やFR (フレームリレー) を使用した専用線上でIP網を構築する方式のように、単一のOSPFドメインで各カスタマ網を接続する重要性は極めて大きいにもかかわらず、図16の方式では、OSPFドメインが分断されてしまうので、単一のOSPFドメインで各カスタマ網を接続することができないという欠点もある。

【 0 0 1 0 】

本発明の目的は、カスタマ網とプロバイダ網との境界においてカスタマノード

とエッジノードとに対して B G P の実装を不要として、負荷の増大を防止した通信装置及び通信制御方法並びにその制御プログラムの記録媒体を提供することである。

【 0 0 1 1 】

本発明の他の目的は、カスタマ網とプロバイダ網との間でのマルチホーミングを構築可能として、信頼性の向上を図った通信装置及び通信制御方法並びにその制御プログラムの記録媒体を提供することである。

【 0 0 1 2 】

本発明の更に他の目的は、O S P F ドメインが分断されてしまうことをなくして、単一の O S P F ドメインで各カスタマ網を接続することが可能な通信装置及び通信制御方法並びにその制御プログラムの記録媒体を提供することである。

【 0 0 1 3 】

【課題を解決するための手段】

本発明によれば、プロバイダ網上にトンネルを形成することにより、複数のカスタマ網間の通信のための仮想専用線 (V P N) を構築するようにした通信システムにおいて、前記トンネルの入出力端に接続されたエッジ通信装置であって、前記カスタマ網内で使用されるルーティングプロトコルを終端する終端手段を含むことを特徴とするエッジ通信装置が得られる。

【 0 0 1 4 】

そして、前記仮想専用線に関する V P N 構築情報と、前記プロバイダ網に接続され予めカプセルアドレスが割り当てられたポートと前記カスタマ網側の各通信装置の I P アドレスとの対応情報とからなるテーブルを更に含み、前記終端手段は、前記カスタマ網から入力されたパケットの宛先アドレスから前記テーブルを検索する検索手段と、この検索されたカプセルアドレスを基に前記パケットをカプセル化して前記プロバイダ網へ送出するカプセル化手段とを有することを特徴とする。

【 0 0 1 5 】

また、前記終端手段は、前記カスタマ網内の I P アドレスの追加やトポロジの変化に応答して前記カスタマ網で生成される制御パケットを受信解読する手段と

、この解読結果に従って前記テーブルのデータ更新を行う手段とを有することを特徴とし、前記カプセル化手段は、同一の仮想専用線に属する他のカスタマ網に対して、前記カプセルアドレスを基に前記制御パケットをカプセル化して送出するようにしたことを特徴とする。

【 0 0 1 6 】

更に、前記終端手段は、前記プロバイダ網から自装置に到着したパケットに対して前記カプセルアドレスが含まれるカプセルを外し、当該パケットに含まれる宛先 I P アドレスを基に前記テーブルから送出先を決定して送出する手段を有することを特徴とし、また前記終端手段は、前記カスタマ網に対する現用インタフェースの障害に応答してこの障害インタフェースに関連する前記テーブル内の情報を削除すると共に、関連する他のエッジ通信装置へ障害通知及び予備インタフェースの通知をなす手段を有することを特徴とする。

【 0 0 1 7 】

更にはまた、前記終端手段は、他のエッジ通信装置からの障害通知に応答して前記障害インタフェースに関連する前記テーブル内の情報を削除すると共に、前記予備インタフェースの通知に応答して前記テーブル内にこの予備インタフェースに関連する情報を追加する手段を有することを特徴とし、前記カスタマ網内で使用されるルーティングプロトコルは、O S P F プロトコルであることを特徴とする。

【 0 0 1 8 】

本発明によれば、プロバイダ網上におけるエッジ通信装置間にてトンネルを形成することにより、複数のカスタマ網間の通信のための仮想専用線（V P N）を構築するようにした通信システムにおける通信制御方法であって、前記エッジ通信装置において、前記カスタマ網内で使用されるルーティングプロトコルを終端する終端ステップを含むことを特徴とする通信制御方法が得られる。

【 0 0 1 9 】

そして、前記エッジ通信装置には、前記仮想専用線に関する V P N 構築情報と、前記プロバイダ網に接続され予めカプセルアドレスが割り当てられたポートと前記カスタマ網側の各通信装置の I P アドレスとの対応情報とからなるテーブル

が設けられており、前記終端ステップは、前記カスタマ網から入力されたパケットの宛先アドレスから前記テーブルを検索する検索ステップと、この検索されたカプセルアドレスを基に前記パケットをカプセル化して前記プロバイダ網へ送出するカプセル化ステップとを有することを特徴とする。

【 0 0 2 0 】

また、前記終端ステップは、前記カスタマ網内の I P アドレスの追加やトポロジの変化に応答して前記カスタマ網で生成される制御パケットを受信解読するステップと、この解読結果に従って前記テーブルのデータ更新を行うステップとを有することを特徴とし、更に前記カプセル化ステップは、同一の仮想専用線に属する他のカスタマ網に対して前記カプセルアドレスを基に前記制御パケットをカプセル化して送出するようにしたことを特徴とする。

【 0 0 2 1 】

更にはまた、前記終端ステップは、前記プロバイダ網から自装置に到着したパケットに対して前記カプセルアドレスが含まれるカプセルを外し、当該パケットに含まれる宛先 I P アドレスを基に前記テーブルから送出先を決定して送出するステップを有することを特徴とし、また前記終端ステップは、前記カスタマ網との現用インタフェースの障害に応答してこの障害インタフェースに関連する前記テーブル内の情報を削除すると共に、関連する他のエッジ通信装置へ障害通知及び予備インタフェースの通知をなすステップを有することを特徴とする。

【 0 0 2 2 】

更に、前記終端ステップは、他のエッジ通信装置からの障害通知に応答して前記障害インタフェースに関連する前記テーブル内の情報を削除すると共に、前記予備インタフェースの通知に応答して前記テーブル内にこの予備インタフェースに関連する情報を追加するステップを有することを特徴とする。また、前記テーブルを集中管理する集中処理装置が設けられており、前記制御パケットの解読結果に従って前記テーブルのデータ更新後に、この更新されたテーブルを前記集中処理装置へアップロードするステップと、前記集中処理装置からこのアップロードされたテーブルに関連するエッジ通信装置にダウンロードするステップとを含むことを特徴とする。

【 0 0 2 3 】

本発明によれば、プロバイダ網上におけるエッジ通信装置間にてトンネルを形成することにより、複数のカスタマ網間の通信のための仮想専用線（VPN）を構築するようにした通信システムにおける通信制御方法のプログラムを記録した記録媒体であって、前記プログラムは、前記エッジ通信装置において、前記カスタマ網内で使用されるルーティングプロトコルを終端する終端ステップを含むことを特徴とする記録媒体が得られる。

【 0 0 2 4 】

本発明の作用を述べる。プロバイダ網とカスタマ網との境界に位置するエッジ通信装置において、カスタマ網でのルーティングプロトコルを終端する構成とする。これにより、カスタマ網とプロバイダ網との境界においてカスタマ通信装置とエッジ通信装置とに対してBGPの実装を不要として、負荷の増大を防止し、またカスタマ網のルーティングプロトコルとして、OSPFプロトコルを使用することで、プロバイダ網との間でのマルチホーミングを構築可能となり、信頼性の向上が図れる。更に、単一OSPFドメインで各カスタマ網を接続することが可能となるものである。

【 0 0 2 5 】

【発明の実施の形態】

以下に、図面を参照しつつ本発明の実施の形態につき詳述する。図1は本発明によるエッジノードを用いて構築したVPN構成を説明するための概略システム構成図であり、図16と同等部分は同一符号により示している。ここで提案されるVPN構築方式は、カスタマノード11～13，21～23，31～33からなるカスタマ網A1～A3と、コアノード44，45とエッジノード41～43とからなるプロバイダ網C1とにより構成されている。

【 0 0 2 6 】

図1におけるカスタマ網A1、カスタマ網A2、カスタマ網A3は、プロバイダ網C1の境界での、すなわちトンネル51や52の両端に位置するエッジノードでのカプセル化処理によるトンネリングにより、VPNを構築している。従って、カスタマ網A1～A3は同一のAS（Autonomous System）に属し、同一の

I G P s (Interior Gateway Protocols)、例えば、R I P (Routing Information Protocol)、O S P F (Open Shortest Path First) により、カスタマノードのトポロジデータベースを更新／管理することができる。尚、本例では、I G P s として O S P F を使用するものとしている。

【 0 0 2 7 】

エッジノード 4 1 ～ 4 3 の各々のカスタマ網側は、接続されたカスタマ網で使われている O S P F プロトコルの終端処理が可能であり、よって図 1 に示すように、カスタマ網 A 1 ～ A 3 は C (Customer) - O S P F が使用可能であり、プロバイダ網 C 1 は V R (VPN ROUTING) - O S P F が使用可能であり、図 1 3 に示したようにカスタマ網とプロバイダ網との間のインタフェース部で使用されていた E B G P を使用する必要がなくなる。すなわち、カスタマ網側の C - O S P F 制御パケットは、プロバイダ網内では、一般の I P パケットとして転送され、トンネルとなるのである。各 C - O S P F はプロバイダ網内の V R - O S P F の存在に気付かないということであり、つまりは、各 C - O S P F は同じ O S P F ドメインに属することになる。これ等を実現する機能として、エッジノードにおいて、終端機能と V R テーブル情報の更新機能とを設けるものである。

【 0 0 2 8 】

また、O S P F では、複数のリンクに対して異なるメトリック値を設定しておき、メトリック値が、例えば小なるリンクを優先的に選択する、いわゆるマルチホーミングが使用可能であるので、カスタマ網とプロバイダ網との間でこのマルチホーミングを構築可能として、信頼性の向上を図り得るのである。

【 0 0 2 9 】

図 2 は本発明の実施例を示すシステム概略図であり、図 1 と同等部分は同一符号にて示している。尚、図 2 では、簡単化のためにコアノードは省略して示している。図 2 に示すように、カスタマ網 A 1 のカスタマノード 1 1 ～ 1 3 のプライベート I P (Internet Protocol) アドレスは “a a”, “a b”, “a c” とし、またカスタマ網 A 2 のカスタマノード 2 1 ～ 2 3 のプライベート I P アドレスは “b a”, “b b”, “b c” とし、更にカスタマ網 A 3 のカスタマノード 3 1 ～ 3 3 のプライベート I P アドレスは “c a”, “c b”, “c c” とする

【 0 0 3 0 】

エッジノード 4 1 ～ 4 3 のプロバイダ網 C 1 側のカプセルアドレスは “ E 1 ” ～ “ E 3 ” とする。そして、エッジノード 4 1 のカスタマ網側のインタフェースのアドレス（プライベート I P アドレス）は “ I 1 1 ” とし、エッジノード 4 2 のカスタマ網側のインタフェースの I P アドレスは “ I 2 1 ” とし、エッジノード 4 3 のカスタマ網側のインタフェースの I P アドレスは “ I 3 1 ” 及び “ I 3 2 ” とする。

【 0 0 3 1 】

そして、本実施例では、前述のマルチホーミングのためのカスタマ網 A 1 内でのトポロジデータベース（ルーティングのためのルーティングテーブル）に対して、2つのプライベート I P アドレス “ I 1 1 ” と “ I 2 1 ” とを、予め提供しておくものとする。カスタマ網 A 1 内でのルーティングプロトコル（O S P F）において、この提供された2つの I P アドレス “ I 1 1 ” , “ I 2 1 ” を経路とするメトリック値の大小を、前者の経路の値がより小となるようにしておくことで、I P アドレス “ I 1 1 ” を経るルーティングである V P N トンネル 5 1 が現用系として選択されるようにすることができる。

【 0 0 3 2 】

図 3 は図 2 におけるエッジノードの概略ブロック図であり、カスタマ網からのパケットを終端処理する終端部 1 と、この終端部の動作制御やルーティングの制御をなす制御部（C P U）2 と、V P N 構築情報及びプロバイダ網に接続され予めカプセルアドレスが割り当てられたポートとカスタマ網の各ノードの I P アドレスとの対応情報を有するテーブル、すなわち V R テーブル 3 と、制御部の動作制御プログラム（ソフトウェア）を予め格納した R O M 4 と、カスタマ網及びプロバイダ網とのインタフェースをなす I / F 部 5 , 6 とを有している。

【 0 0 3 3 】

図 4 はエッジノード 4 1 ～ 4 3 が夫々有するルーティング制御のための V R テーブルの概念図を示しており、V R テーブルは同じ V P N I D（V P N 識別情報）を持っていてもそれが格納されるエッジノードによりその内容は相違してお

り、図4に示すように、エッジノード41はVR IDとして“11”，“12”，“13”，……に夫々対応するVRテーブルを有しており、VR ID “11” の具体例（図2に対応）が図5に示されている。また、エッジノード42はVR IDとして“21”，“22”，“23”，……に夫々対応するVRテーブルを有しており、VR ID “21” の具体例（図2に対応）が図6に示されている。更に、エッジノード43はVR IDとして“31”，“32”，“33”，……に夫々対応するVRテーブルを有しており、VR ID “31” の具体例（図2に対応）が図7に示されている。

【0034】

これ等VRテーブルはカスタマ網側インタフェース（INF）の関連付け情報を含んでおり、これはIP-VPNサービスをプロバイダ網に申し込む際に登録されるもので、カスタマ網側でプライベートアドレスが使用できるようにするための不可欠な情報である（異なるカスタマ網で同じアドレスが存在し得る場合があり、この場合どのカスタマ網側インタフェースから入力されてきたかでVRテーブルを識別するものである）。また、Egress（出力）エッジノードのカスタマ側インタフェースの状態、つまりそのカプセル化アドレスが有効であるかどうかの情報（OK/NG）をも含んでいる。

【0035】

更に、VPN IDをも含んでいる。このVPN IDはそのVRテーブルを使用するカスタマに付与されたグローバルユニークな情報である。VRテーブルは同じVPN IDを持っていたとしても、それが格納されるエッジノードにより相違するものである（図4参照）。また、カプセル化アドレスの優先度をも含み、この優先度は先述したメトリック値に相当するものであって、優先度“1”（現用系）が“2”（予備系）よりも優先するものとする。

【0036】

図8は本発明の実施例の動作を示すシーケンス図であり、カスタマ網からのパケット転送時と、カスタマ網でのアドレス変更時と、メトリック小（現用系）のリンク断時との、各場合におけるものである。先ず、カスタマ網からのパケット転送時について、図9のフローチャートをも参照しつつ説明する。例えば、カス

タマ網 A 1 のノード 1 2 から他のカスタマ網 A 2 のノード 2 2 へパケット転送要求があるとする（ステップ S 1）。このときのパケットは、図 1 0（A）に示すように、そのヘッダ部分に、送信元アドレス／宛先アドレスとして、a b／b b が表記されている。

【 0 0 3 7 】

カスタマ網 A 1 内での O S P F ルーティングプロトコルに従って当該パケットはノード 1 1 を経て、メトリック値が小のリンクが自動的に選択されてエッジノード 4 1 へ供給される。エッジノード 4 1 では、終端処理が行われる。すなわち、そのパケットの転送先を解決すべく、先ずこのパケットが入力されてきたカスタマ網側インタフェース I 1 1 から定まる V R テーブル（1 1）を得る（ステップ S 2）。この V R テーブル（1 1）から網内パケットに含ませるべき V P N I D（1）を得る（ステップ S 3）。

【 0 0 3 8 】

次に、宛先プライベートアドレス（b b）と、E g r e s s エッジノードのカスタマ側 I N F 状態（O K）を元に、カプセル化アドレス（E 3）を解決し（ステップ S 4）、図 1 0（B）に示すように、V P N I D と送信元カプセル化アドレス／宛先カプセル化アドレスである E 1／E 3 とがヘッダに付加されて、カプセル化が行われる（ステップ S 5）。このカプセル化されたパケットは対応する出力 I N F（プロバイダ網側）へ網内パケットとして転送される（ステップ S 6）。

【 0 0 3 9 】

このカプセルを受信したエッジノード 4 3 での動作を図 1 1 のフローチャートに示している。エッジノード 4 3 では、このカプセルを終端部 1 で受信して（ステップ S 1 1）、当該網内パケット転送先を解決するために、先ず当該パケットが持つ V P N I D を元に、V R テーブル（3 1）を得て、この V R テーブル（3 1）内で、宛先プライベート I P アドレス（b b）を元に、対応する出力 I N F（I 3 1）を決定する（ステップ S 1 2）。そして、図 1 0（C）に示すように、カプセル化アドレスと V P N I D とをヘッダから外して逆カプセル化を行い（ステップ S 1 4）、送信する（ステップ S 1 5）。

【 0 0 4 0 】

カスタマ網内のアドレスが変更された場合の動作を、図 1 2 のフローチャートを参照して説明する。あるカスタマ網のあるノードの I P アドレスが変更になると、その変更を通知するための制御パケットが網内で転送され（Hello プロトコル等を使用して）、対応するエッジノードにも送信される（ステップ S 2 1）。

【 0 0 4 1 】

この制御パケットのヘッダ部には、このパケットが制御パケットである旨を示す情報が予め付加されているので、この情報により終端部 1 は制御パケットの認識が可能であり、この制御パケットにのせられているアドレス変更の情報を解読して、V R テーブルの内容の更新を行う（ステップ S 2 2）。そして、プロバイダ網内における V R テーブルの情報の交換をなすための交換プロトコルを使用して、関連するエッジノードに対して、アドレス変更の通知を行う（ステップ S 2 3）。

【 0 0 4 2 】

現用トンネルに対応するインタフェースのリンク（メトリック値が小）が断になった場合における動作を、図 1 3 のフローチャートを使用して説明する。図 2 に示したメトリック値が小のリンクが断になると、その障害を通知するための制御パケットが網内で転送される（Hello プロトコル等を使用して）ので、各カスタマノードでは、トポロジ D B （データベース）が更新される。

【 0 0 4 3 】

このとき、障害リンクに接続されているエッジノード 4 1 では、障害発生が検出され（ステップ S 3 1）、V R テーブルから断リンクに関連する情報が削除される（ステップ S 3 2）。この場合の削除の方法としては、V R テーブル内の E g r e s s 側のカスタマ網 I N F 状態が、N G に設定されることでなされる。これにより、トンネル 5 1 に関する情報はテーブルから削除されたことと等価になる。そして、交換プロトコルにより関連するエッジノードに対して同様に削除通知の他に、メトリックの小なるリンクがアクティブになる旨の通知がなされる（ステップ S 3 3）。

【 0 0 4 4 】

次に、図 1 4 のフローチャートを参照すると、図 1 1 のステップ S 3 3 による通知を受けた場合（ステップ S 4 1）、その V R テーブルから断リンクに関する情報が削除される（ステップ S 4 2）。同時に、メトリックの大なるリンクがアクティブになる旨の通知により、V R テーブルに対して、このメトリックの大的リンクに関する情報が追加される（ステップ S 4 3）。

【 0 0 4 5 】

ここで、I G P s として O S P F を想定した場合、現用系として使用したいエッジ通信網に対してメトリック値を小さく設定し、他方のメトリック値は大きく設定しておく（V P N のメトリック値には、プロバイダ網内の経路を反映する方式と、しない方式とが考えられるが、ここでは、プロバイダ網内の経路から算出されるメトリック値は V P N のメトリック値に反映しないこととする。従って、図 2 の様なマルチホーミング構成では、メトリック値に大差をつける必要はなく、大小の関係が成立すればよい）。

【 0 0 4 6 】

カスタマ網内のアドレスやトポロジの変更に伴う V R テーブルの更新には、プロバイダ網内で I B G P を使う前述した方式と、集中型処理装置を介して更新する方式とが考えられる。図 1 5 はこの集中型処理装置を使用した方式の例であり、図 2 と同等部分は同一符号にて示している。この例では、集中処理装置 1 0 0 が一方のエッジノードから V P N 構築情報をアップロードし、しかる後に関係するエッジノード内 V R テーブルにダウンロードすることが考えられる。

【 0 0 4 7 】

【発明の効果】

本発明によれば、カスタマノードは、B G P をサポートする必要はなく、I G P のみで V P N が構築できるという効果がある。また、カスタマノードが複数のエッジノードに接続されるマルチホーミング構成を、B G P を使用することなく構成することができ、V P N の信頼性を向上させることができるという効果もある。更に、O S P F ドメインの分断がなくなり、A T M や F R を使用した専用線上で I P 網を構築する方式のように、単一 O S P F ドメインで、各カスタマ網を接続できるという意義は大である。

【図面の簡単な説明】

【図 1】

本発明の基本構成を示すシステムブロック図である。

【図 2】

本発明の実施例を示すシステムブロック図である。

【図 3】

本発明のエッジノードの機能を示す概略図である。

【図 4】

エッジノードにおける V R テーブルとプロバイダ網側インタフェースとの関係を示す概念図である。

【図 5】

V R テーブルの内容の一例を示す図である。

【図 6】

V R テーブルの内容の一例を示す図である。

【図 7】

V R テーブルの内容の一例を示す図である。

【図 8】

本発明の実施例の動作を説明するためのシーケンス図である。

【図 9】

本発明の実施例におけるパケット転送時の動作を示すフローである。

【図 1 0】

カプセル化及び逆カプセル化を説明するための図である。

【図 1 1】

本発明の実施例におけるカプセル受信時の動作を示すフローである。

【図 1 2】

本発明の実施例における制御パケット受信時の動作を示すフローである。

【図 1 3】

本発明の実施例における現用リンク障害時の動作を示すフローである。

【図 1 4】

本発明の実施例における予備リンクアクティブ時の動作を示すフローである。

【図 1 5】

本発明の他の実施例の概略システムブロック図である。

【図 1 6】

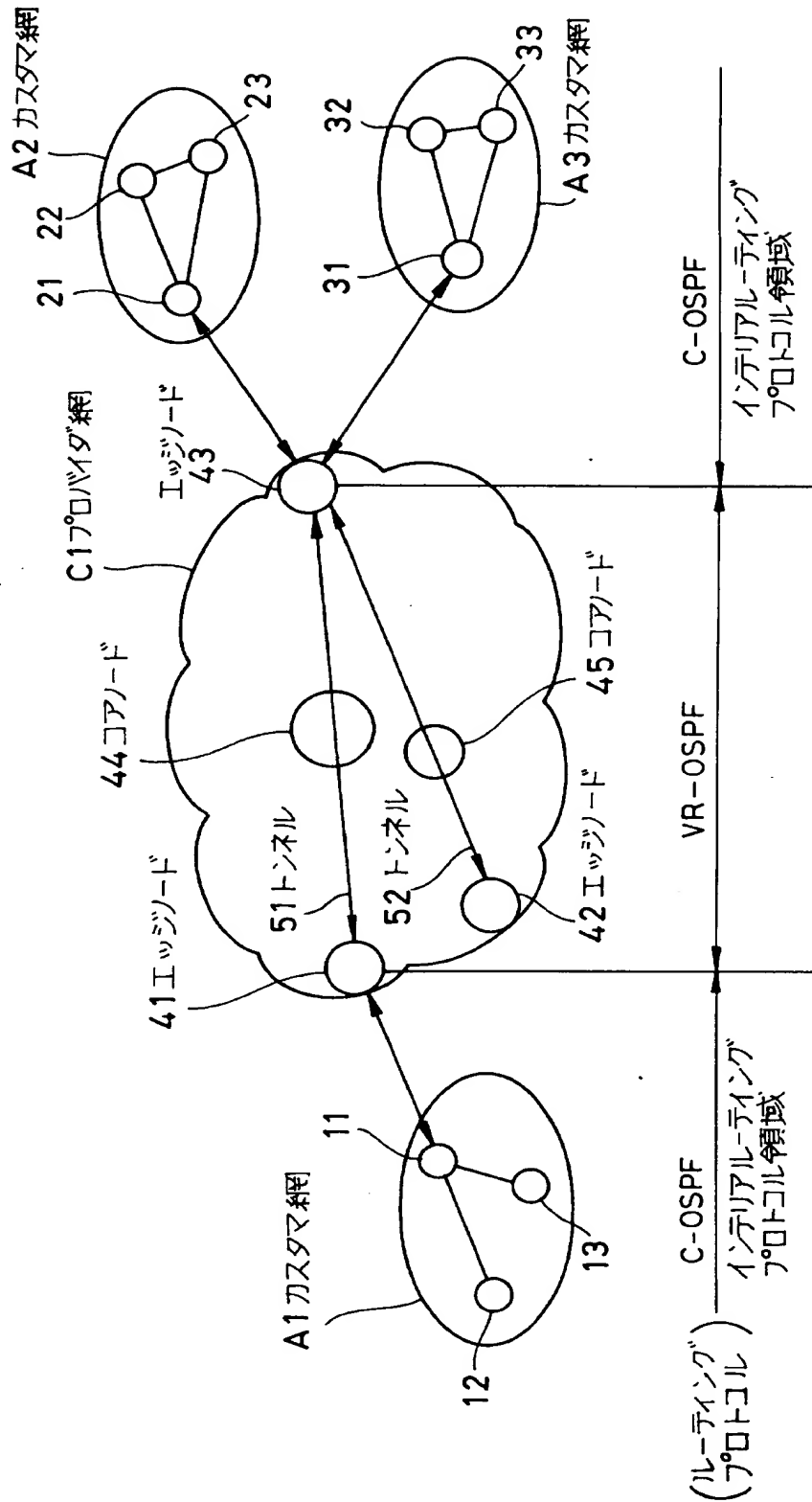
従来技術を説明するための概略システムブロック図である。

【符号の説明】

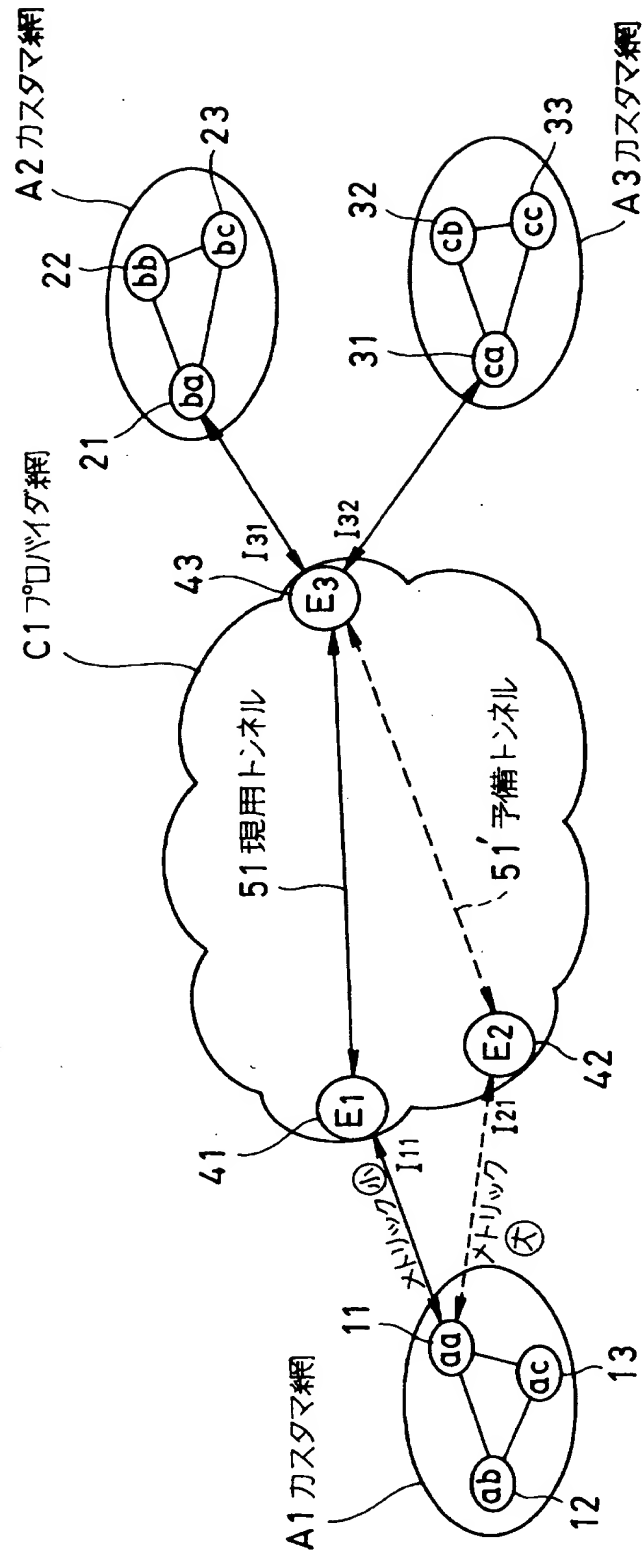
- A 1 ～ A 3 カスタマ網
- C 1 プロバイダ網
- 1 終端部
- 2 制御部
- 3 V R テーブル
- 4 R O M
- 5, 6 インタフェース部
- 1 1 ～ 1 3, 2 2 1 ～ 2 3,
- 3 1 ～ 3 3 カスタマノード
- 4 1 ～ 4 3 エッジノード
- 5 1 現用トンネル
- 5 1 ' 予備トンネル
- 1 0 0 集中処理装置

【書類名】 図面

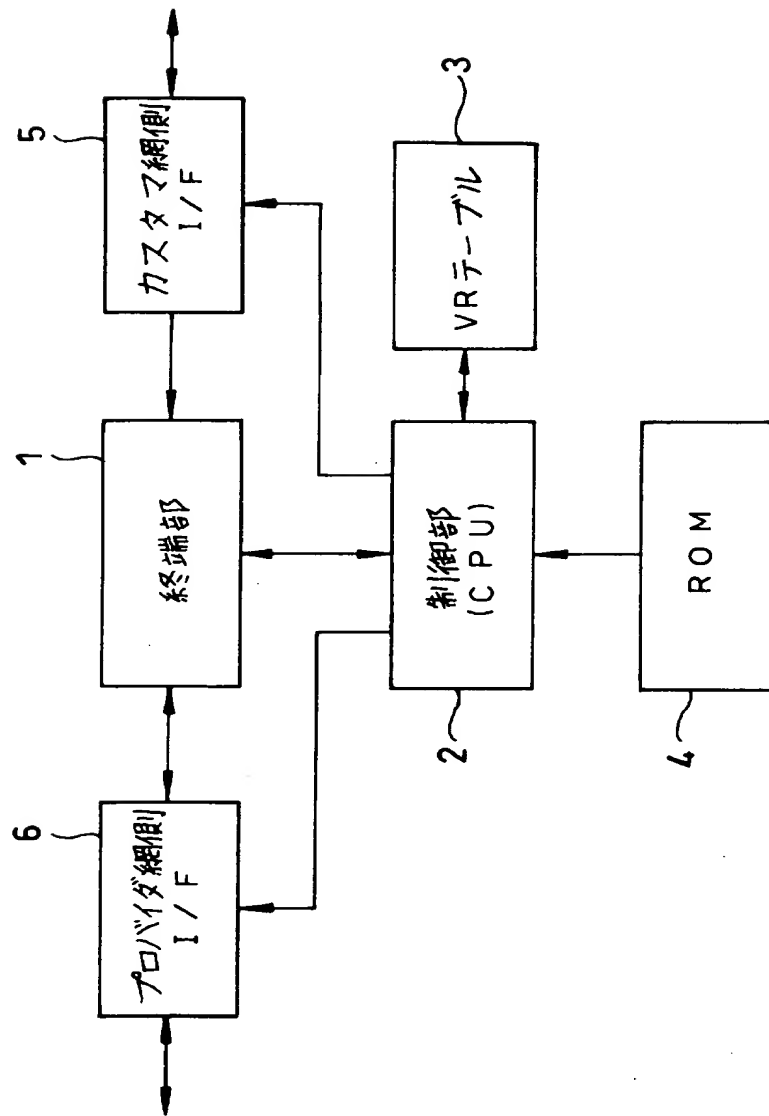
【図 1】



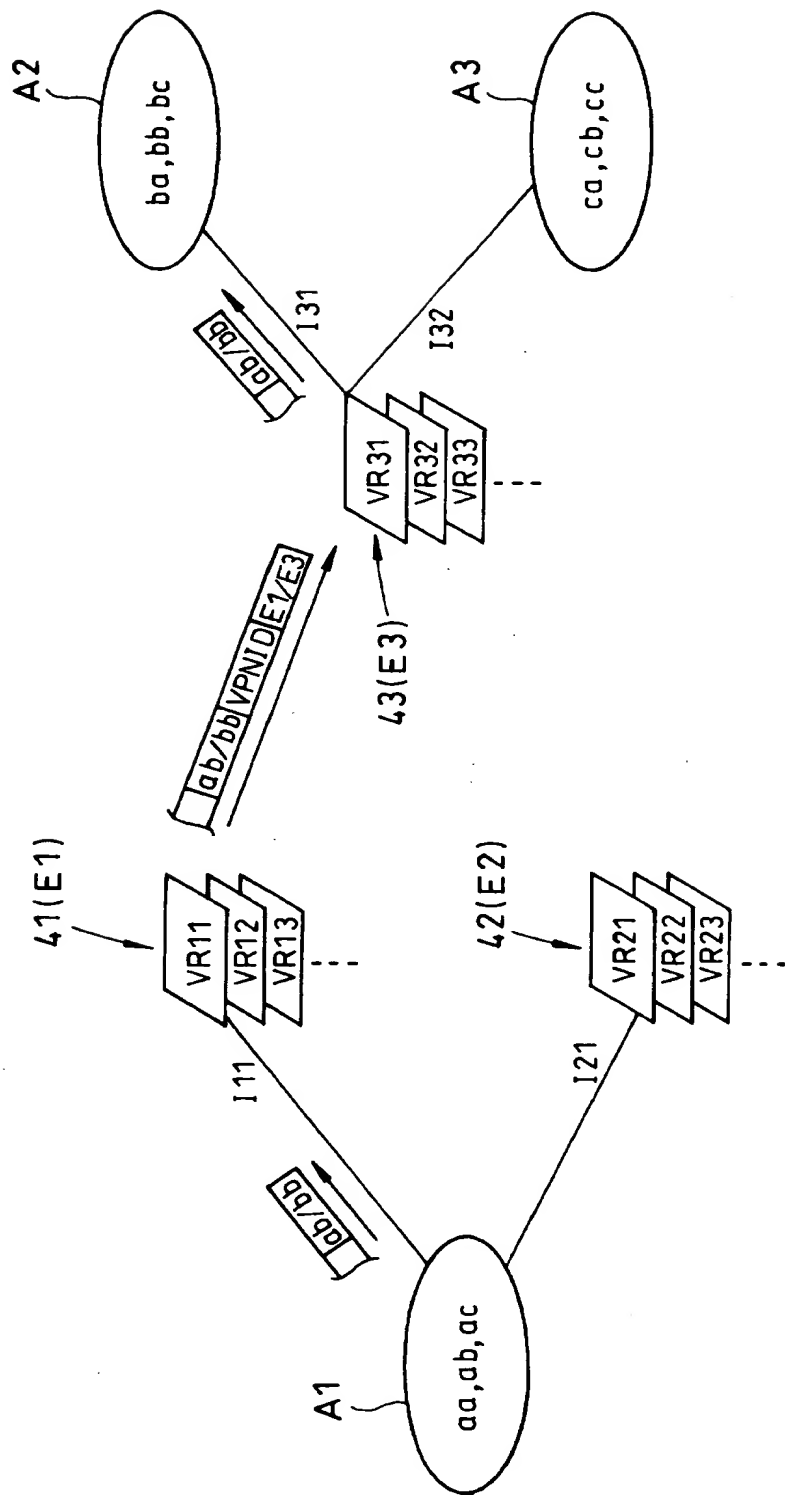
【図2】



【図 3】



【図 4】



【図 5】

41(E1)のVRテーブル

VR テー ブル ID	カスタム側 INF	VPN ID	宛先 プライベート アドレス	カプセル化 アドレス	Egress エッジ のカスタム側 INF 状態	VRからの 出力INF	カプセル化 アドレスの 優先度
11	I11	1	aa	—	—	I11	—
			ab	—	—	I11	—
			ac	—	—	I11	—
			ba	E3	OK/NG	プロバイダ側	1
			bb	E3	OK/NG	プロバイダ側	1
			bc	E3	OK/NG	プロバイダ側	1
			ca	E3	OK/NG	プロバイダ側	1
			cb	E3	OK/NG	プロバイダ側	1
			cc	E3	OK/NG	プロバイダ側	1

【図 6】

42 (E2) の VR テーブル

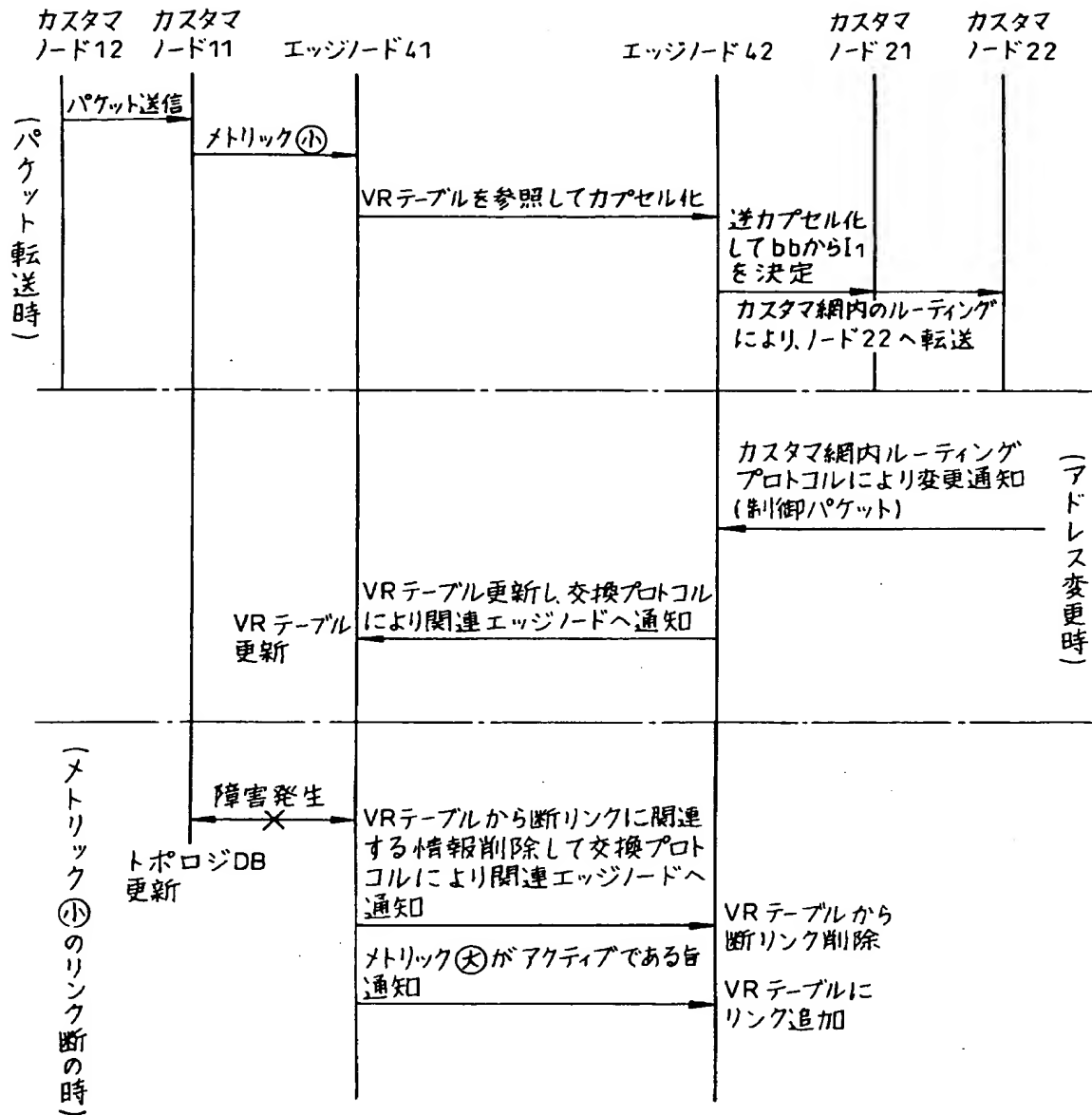
VR テーブル ID	カスタマ側 INF	VPN ID	宛先 プライベート アドレス	カプセル化 アドレス	Egress エッジ のカスタマ側 INF 状態	VR からの 出カ INF	カプセル化 アドレスの 優先度
21	I21	1	aa	—	—	I21	—
			ab	—	—	I21	—
			ac	—	—	I21	—
			ba	E3	OK/NG	プロバイダ側	1
			bb	E3	OK/NG	プロバイダ側	1
			bc	E3	OK/NG	プロバイダ側	1
			ca	E3	OK/NG	プロバイダ側	1
			cb	E3	OK/NG	プロバイダ側	1
			cc	E3	OK/NG	プロバイダ側	1

【図 7】

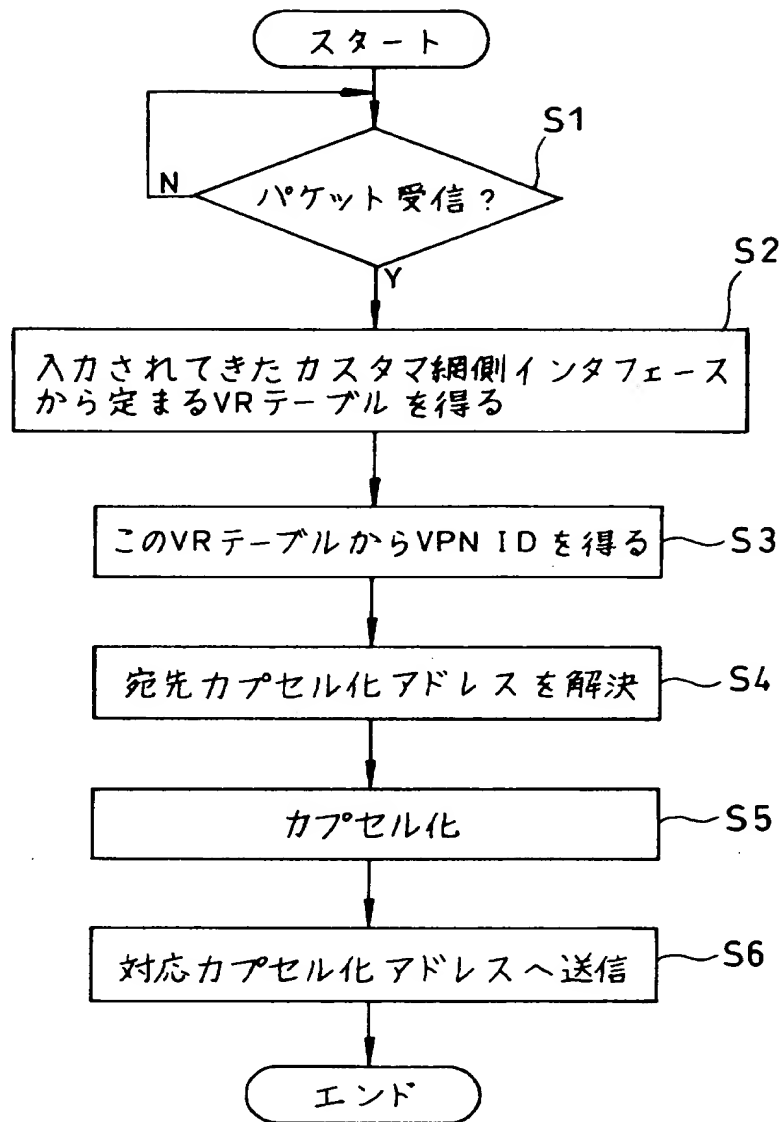
43(E3)のVRテーブル

VR テーブル ID	カスタマ側 INF	VPN ID	宛先 プライベート アドレス	カプセル化 アドレス	Egress エッジ のカスタマ側 INF 状態	VR からの 出カ INF	カプセル化 アドレスの 優先度
31	I31	1	aa	E 1	OK/NG	プロバイダ側	1
				E 2	OK/NG	プロバイダ側	2
			ab	E 1	OK/NG	プロバイダ側	1
				E 2	OK/NG	プロバイダ側	2
			ac	E 1	OK/NG	プロバイダ側	1
				E 2	OK/NG	プロバイダ側	2
	I32		ba	—	—	I31	—
				—	—	I31	—
			bc	—	—	I31	—
				—	—	I32	—
			ca	—	—	I32	—
				—	—	I32	—
			cb	—	—	I32	—
				—	—	I32	—

【図 8】

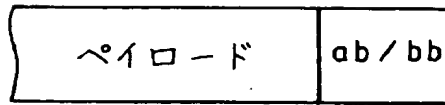


【図 9】



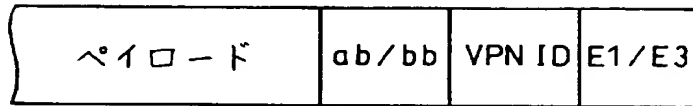
【図 1 0】

(A)



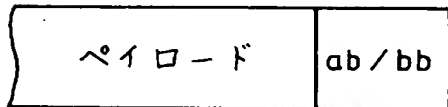
↓ (カプセル化)

(B)

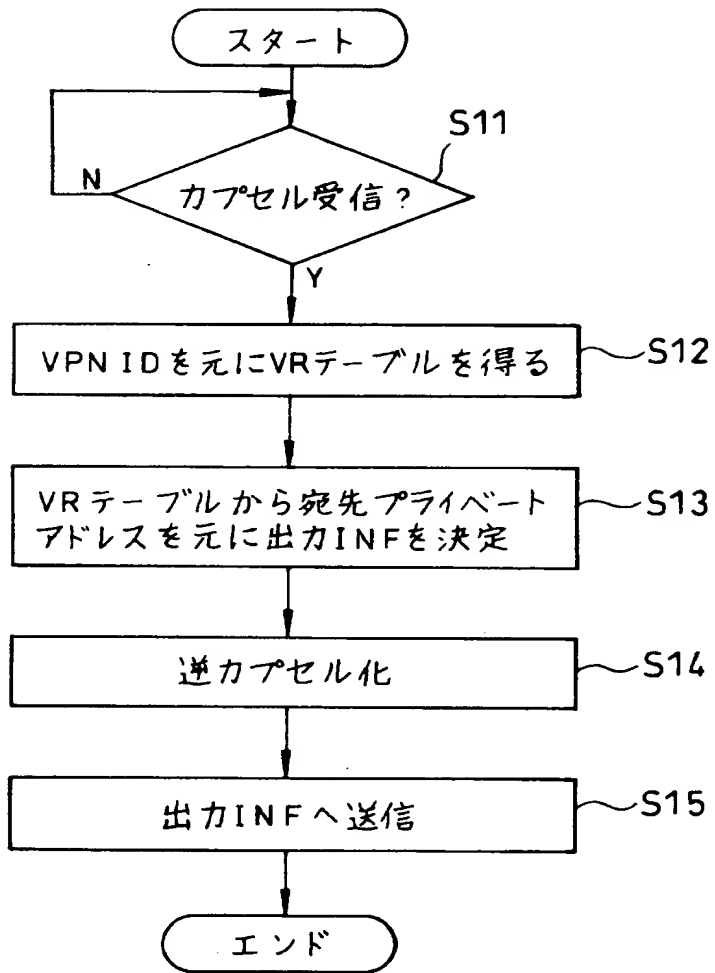


↓ (逆カプセル化)

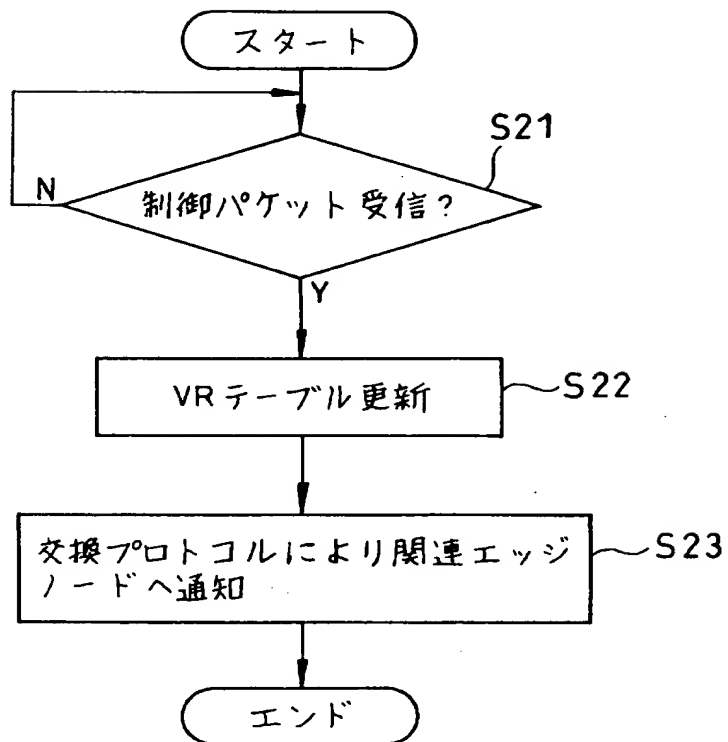
(C)



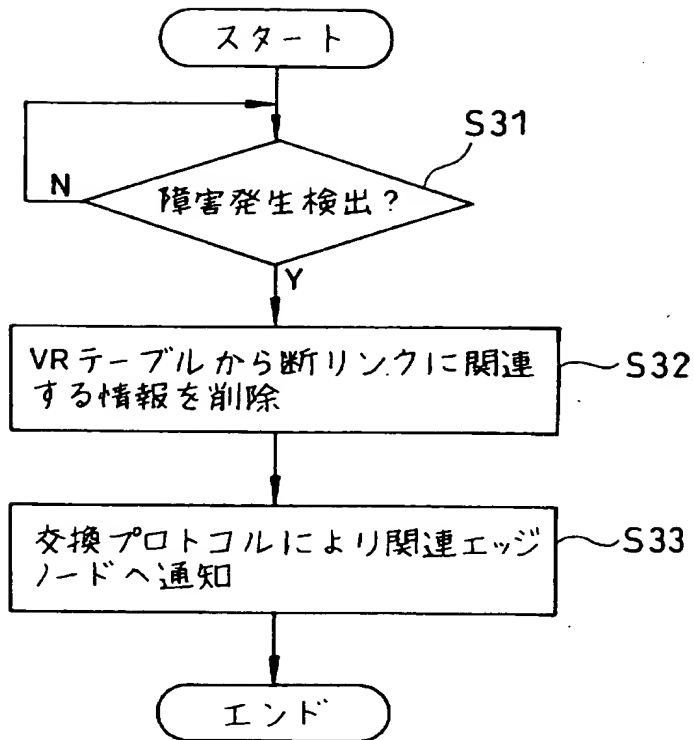
【図 1 1】



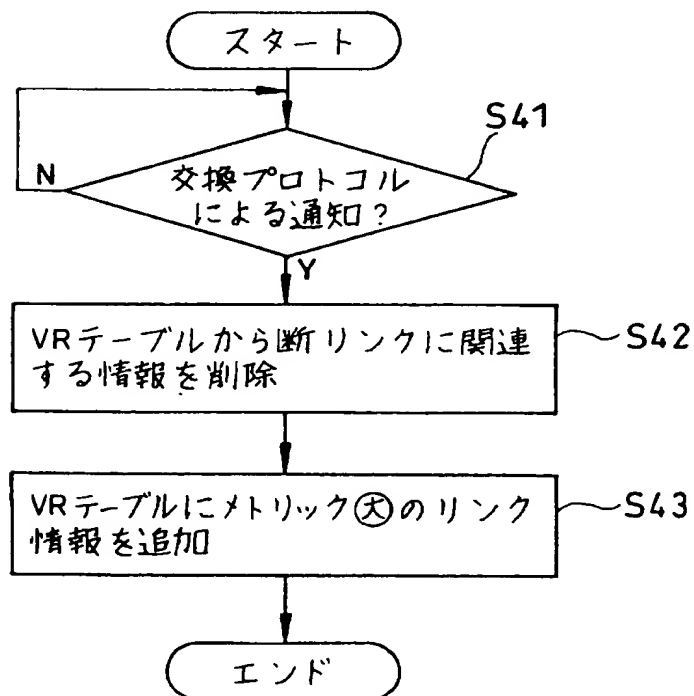
【図 1 2】



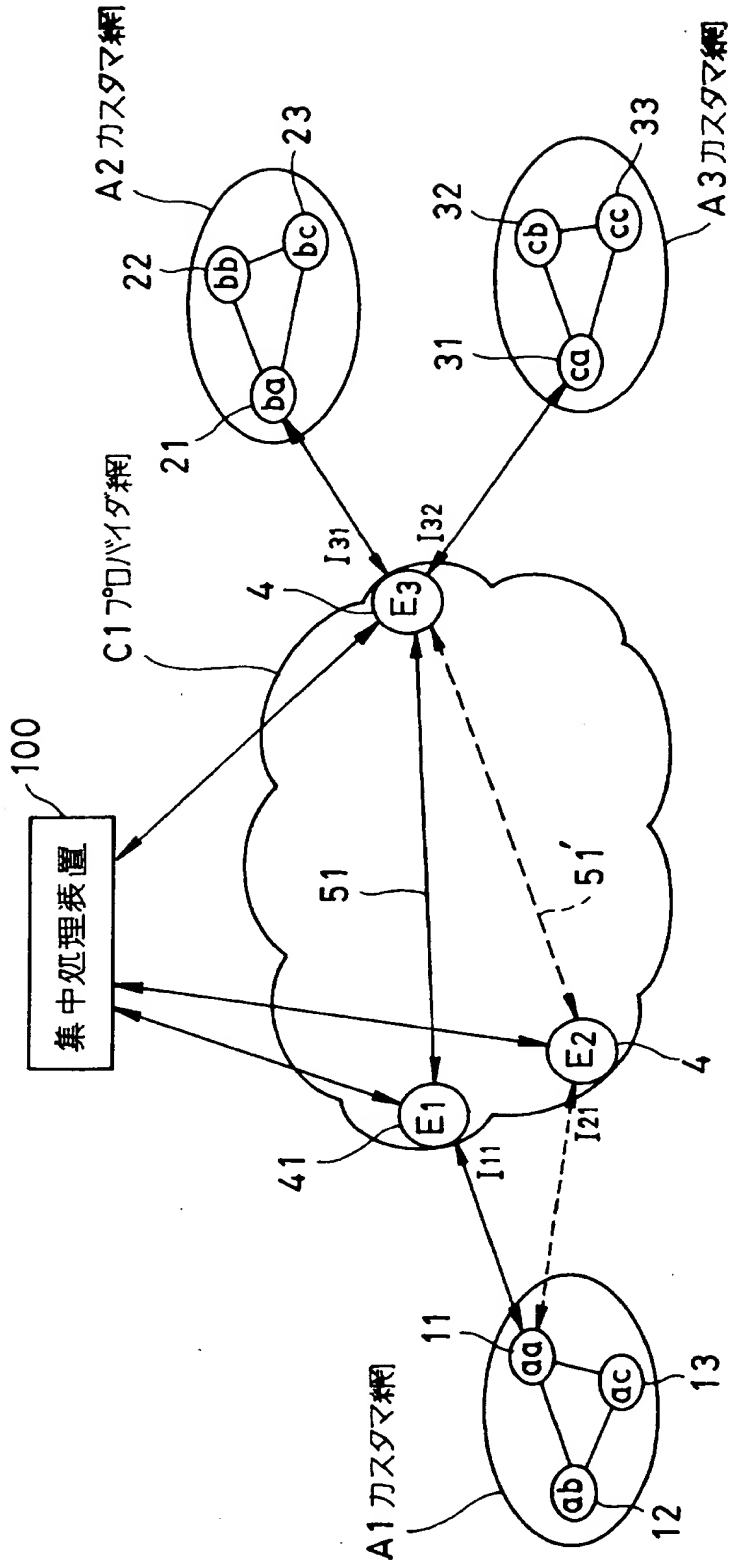
【図 1 3】



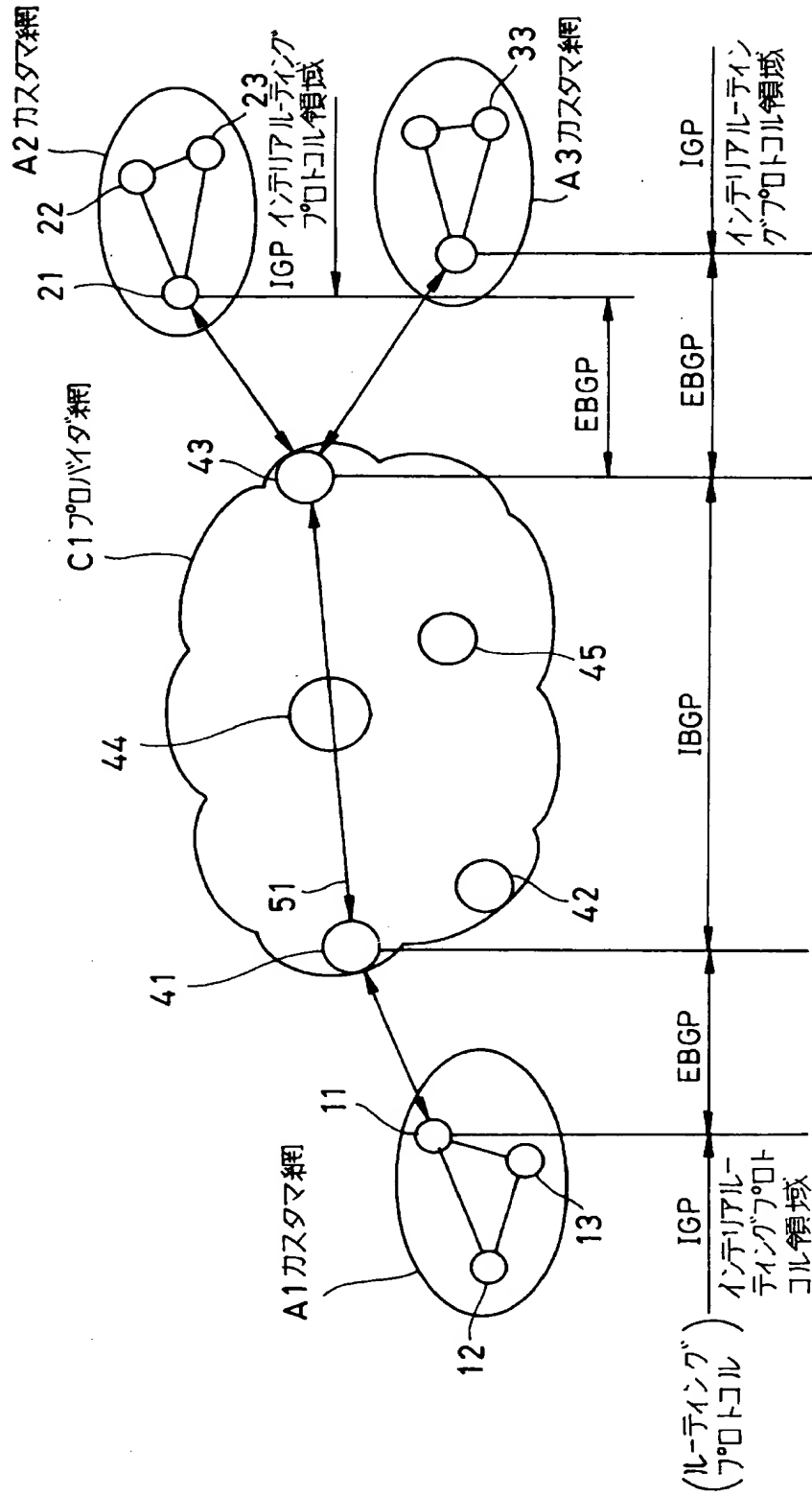
【図 1 4】



【図15】



【図 16】



【書類名】 要約書

【要約】

【課題】 カスタマ網とプロバイダ網との境界においてカスタマ通信装置とエッジ通信装置とに対して B G P の実装を不要として、負荷の増大を防止した通信装置及びそれを使用した通信システムを得る。

【解決手段】 複数のカスタマ網 A 1 ～ A 3 と、トンネル化技術を利用したプロバイダ網 C 1 からなる V P N において、カスタマ網とプロバイダ網との境界に位置するエッジノード 4 1 ～ 4 3 に、カスタマ網内の I G P s (Interior Gateway Protocols) を終端する機能を設ける。これにより、カスタマ網とプロバイダ網との境界においてカスタマノードとエッジノードとに対して、B G P (Border Gateway Protocol) の実装が不要となる。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000004237]

1. 変更年月日	1990年 8月29日
[変更理由]	新規登録
住 所	東京都港区芝五丁目7番1号
氏 名	日本電気株式会社